

INTERNAL POLICY:

INFORMATION SECURITY AND OPERATIONAL GOVERNANCE

- **Document Identifier:** AENV-ISMS-POL-001
- **Issuing Authority:** Office of the Chief Compliance Officer & CISO, Aquarius Entertainment N.V.
- **Effective Date:** August 18, 2026
- **Version:** 3.0 (Comprehensive Governance & Strategic Principles Edition)
- **Scope:** All departments, employees, contractors, consultants, and third-party vendors of Aquarius Entertainment N.V.

1. OVERVIEW, REGULATORY MANDATE, AND GOVERNANCE PRINCIPLES

1.1 Legislative Basis and Authority

This policy document establishes the mandatory Information Security Management System (ISMS) framework for Aquarius Entertainment N.V. (the "Company"). This policy is promulgated pursuant to the statutory compliance obligations mandated under the *Landsverordening op de Kansspelen* (LOK) and the *Landsverordening Casinowezen Curaçao* (LCC), as regulated and enforced by the Curaçao Gaming Authority (CGA).

PDF

1.2 Regulatory Accountabilities and Non-Delegable Responsibility

Compliance with the controls outlined within this policy constitutes a non-negotiable, mandatory condition of licensure under LOK Article 5.

PDF

The Company explicitly recognizes that while technical operations, game engines, sports feeds, or cloud infrastructure may be contractually delegated, hosted, or managed by third-party B2B providers, game aggregators, or managed service providers (MSPs), **the Company retains ultimate, non-delegable legal and regulatory accountability under the LOK.** Contractual delegation does not transfer regulatory risk. The Company is obligated to enforce continuous due diligence, technical verification, and audit oversight over all external ecosystems.

1.3 Overarching Information Security Principles (Strategic Directives)

All technical architecture, operational procedures, software development lifecycles, and administrative decisions within the Company must adhere to the following eight core strategic principles:

I. Principle of Zero Trust Architecture (Never Trust, Always Verify)

The Company operates under a strict Zero Trust posture across all network zones. No user, endpoint, workload, or network interface—whether internal, external, or cloud-hosted—shall be implicitly trusted based on network location or organizational hierarchy. Every access request to corporate systems or gaming databases must be explicitly authenticated, authorized based on dynamic risk scores, and encrypted prior to granting access.

II. Principle of Defense-in-Depth (Layered Security Controls)

Security controls must never rely on a single point of defense. The Company enforces a layered security architecture encompassing physical security, perimeter boundaries, network segmentation, host hardening, endpoint protection, application-level security, identity governance, and continuous data-at-rest encryption. The failure or compromise of a single control layer must not compromise the integrity of the overall enterprise.

III. Principle of Least Privilege and Separation of Duties (SoD)

Identity and access management must strictly enforce the principle of least privilege. Users, service accounts, and system processes are granted only the absolute minimum system permissions required to perform their designated business functions. High-risk administrative actions, financial disbursements, system schema modifications, and regulatory compliance changes must require dual authorization (four-eyes principle) and strict separation of duties to mitigate insider threats and administrative error.

IV. Principle of Privacy by Design and Default (PbD)

Data protection and privacy controls must be embedded into the system architecture from the initial conceptual design phase through development, testing, and deployment. The default settings for all player-facing platforms, internal databases, and employee tools must enforce the highest level of privacy restrictions. Personal data

ta (PII) collection must be strictly limited to what is necessary for regulatory compliance (KYC/AML) and core gaming functionality.

V. Principle of Immutable Traceability and Non-Repudiation

All critical gaming operations, administrative escalations, random number generation (RNG) outputs, financial transfers, and security events must generate persistent, tamper-proof audit trails. System architectures must ensure non-repudiation-guaranteeing that every system action, transaction, or configuration change can be unequivocally attributed to a verified identity, timestamp, and source address.

PDF

VI. Principle of Operational Resilience and Disaster Survivability

Information security is fundamentally integrated with business continuity. Technical systems supporting core wagering, player balances, and regulatory reporting must be architected with high availability, redundant fault domains, and automated failover capabilities. Operational infrastructure must be engineered to withstand, absorb, and rapidly recover from security incidents, hardware failures, localized disasters, or malicious cyberattacks without catastrophic data loss.

PDF+ 1

VII. Principle of Proportionality and Risk-Based Security Governance

Security measures and investments shall be deployed proportionately, calibrated against the specific threat landscape, asset criticality, and potential impact on gaming integrity or regulatory standing. Risk assessments must be conducted dynamically to ensure that security controls effectively mitigate operational risks without imposing unreasonable, non-value-added operational overhead on business functions.

PDF

VIII. Principle of Continuous Compliance and Audit-Readiness

Compliance is not a periodic event; it is a continuous operational state. All technological environments, administrative procedures, and third-party integrations must remain permanently audit-ready. The Company shall maintain continuous automated monitoring, periodic technical assessments, and documented evidence repositories to demonstrate compliance to the CGA, external auditors, and law enforcement agencies upon demand.

PDF

2. CORE OPERATIONAL REQUIREMENTS AND TECHNICAL PROCEDURES

2.1 Enterprise Asset and Software Lifecycle Management

1. **Automated Inventory Discovery:** IT Operations shall maintain an active Configuration Management Database (CMDB) covering all physical servers, virtual instances, containerized workloads, network appliances, and workstations. Automated discovery scripts (utilizing platforms such as Snipe-IT or cloud-native asset inventories) must scan corporate subnets and VPCs daily.

PDF

2. **Bi-Annual Reconciliation:** On the final business day of June and December, the IT Infrastructure Manager and the CISO must execute a full physical and logical asset reconciliation, signing an official *Asset Inventory Reconciliation Certificate*.

PDF

3. **Rogue Device Isolation:** Network Access Control (NAC) utilizing 802.1X authentication and MAC address whitelisting shall be enforced. Weekly automated scans must flag unmanaged hardware. Any unauthorized device detected on corporate subnets must be instantly routed to an isolated Quarantine VLAN, triggering an automated alert to the Security Operations Center (SOC).

PDF+ 1

4. **Software Support Validation & EOL Controls:** IT Operations shall verify the vendor support status of all active operating systems, middleware, and database engines on the 1st of every month. Unsupported or End-of-Life (EOL) software must be decommissioned. If business continuity requires temporary retention, an *Asset Risk Exception Request* must be signed by the CISO, implementing strict network segment isolation for a period not exceeding 90 days.

PDF+ 2

2.2 Sensitive Data Protection, Privacy, and Cryptography

1. **Data Classification Scheme:** All corporate and customer data assets must be categorized into one of four sensitivity tiers:

PDF

- **Critical Gaming Data:** RNG seeds, game event outcomes, financial transaction ledgers, jackpot triggers.

PDF

- **Regulated Personal Data (PII):** Player identity documents, KYC verification records, payment details, Responsible Gaming intervention logs.

PDF

- **Business Confidential:** Proprietary source code, financial statements , strategic operational plans.
PDF
 - **Public Data:** Marketing materials, public website content.
PDF
2. **Endpoint Encryption Controls:** Full-Disk Encryption (FDE via BitLocker for Windows or FileVault for macOS) is mandatory across 100% of enterprise laptops and mobile devices handling corporate or regulated data. Mobile Device Management (MDM) policies must automatically block unencrypted endpoints from accessing corporate Workspace or VPN environments.
PDF
 3. **Cryptographic Key Management:** Production encryption keys must reside in dedicated Cloud Key Management Services (KMS) or Hardware Security Modules (HSM) utilizing AES-256 or RSA-4096 standards. KMS policies must enforce automatic annual key rotation. Embedding hardcoded cryptographic keys within application source code or Git repositories is grounds for immediate termination.
PDF
 4. **Certified Data Sanitization:** Expired data assets and decommissioned storage media must undergo sanitization via cryptographic erasure or physical destruction in compliance with NIST SP 800-88 standards. The CISO must review and retain a signed *Certificate of Sanitization* for all disposed assets.
PDF

2.3 Secure Baseline Configurations and System Hardening

1. **Infrastructure as Code (IaC) Baselines:** All production servers, database clusters, and networking hardware must be provisioned using automated IaC templates (e.g., Ansible, Terraform) pre-configured to CIS Benchmark Level 1 standards. Default vendor passwords, unnecessary system services, and legacy cipher suites must be disabled prior to production deployment.
PDF+ 1
2. **Automated Inactivity Lockouts:**
 - **Workstations:** Group Policies (GPO/MDM) must enforce a mandatory screen saver lockout after **15 minutes** of inactivity, requiring user re-authentication.
PDF
 - **Mobile Devices:** MDM policies must enforce a screen lockout after **2 minutes** of inactivity, configured to execute a local device wipe after 10 consecutive failed passcode attempts.
PDF

3. **Secure Administrative Protocols:** Insecure or plain-text management protocols (including HTTP, Telnet, and FTP) are prohibited across all environments. Administrative access must exclusively utilize encrypted channels (SSH, SFTP, HTTPS) routed through a Bastion Host over an authenticated VPN with Multi-Factor Authentication.

PDF+ 1

2.4 Account Lifecycle and Credential Governance

1. **Account Registry and Quarterly Reconciliation:** IT Operations and HR must maintain a unified Identity and Access Management (IAM) directory. IT Operations shall conduct quarterly access reviews to cross-reference active accounts against current HR employee registries. Orphaned or unassigned accounts must be purged within 24 hours of discovery.

PDF+ 1

2. **Password Complexity Standards:**

- **Accounts with MFA:** Minimum 8 characters incorporating uppercase, lowercase, and numeric characters.

PDF

- **Accounts without MFA (System Accounts):** Minimum 14 characters generated via high-entropy randomness algorithms.

PDF

- All employees shall be provisioned with an enterprise password manager (e.g., 1Password Business). Reusing corporate passwords across external personal services is strictly forbidden.

3. **Dormant Account Disablement:** An automated IAM background process shall evaluate last-login timestamps daily. Accounts showing no login activity for 45 consecutive days shall be automatically set to Disabled status, alerting the department manager.

PDF

4. **Separation of Privileged Accounts:** System administrators shall be issued dual accounts: a standard user account (`username@aquarius.com`) for daily communication and an elevated administrative account (`adm-username@aquarius.com`) reserved strictly for technical maintenance. Administrative accounts must not be provisioned with external email or web-browsing capabilities.

PDF+ 1

2.5 Provisioning Workflows and Multi-Factor Authentication (MFA)

1. **Ticket-Based Access Requests:** All grants, modifications, or elevations of access rights require an audited ticket (e.g., Jira Service Management) containing documented written approvals from the employee's direct manager and

the specific System Owner.

PDF

2. **Termination Offboarding SLA:** HR termination notices shall automatically trigger an offboarding workflow within the IAM system. Upon the effective hour of employee departure, the system must execute an automated script to invalidate all active web sessions, revoke OAuth tokens, and disable directory credentials.

PDF

3. **Mandatory MFA Enforcement:** MFA utilizing Time-based One-Time Password (TOTP) authenticators or FIDO2 hardware security keys is mandatory across:

PDF

- All remote access entry points (VPN, RDP, SSH Bastions, Cloud Consoles).

PDF

- All administrative back-office portals managing core gaming engines, player accounts, or financial transactions.

PDF

- **Standalone SMS-based OTP is strictly prohibited as a sole MFA factor**

.

2.6 Vulnerability Governance and Patch Management

1. **Scanning Cadence:** Automated vulnerability scans covering internal networks, public IP ranges, web applications, and database infrastructure must be conducted on the 15th day of every month using certified scanning platforms (e.g., Nessus, Tenable, Qualys).

PDF

2. **Remediation SLAs:**

- **Critical Risk (CVSS ≥ 9.0):** Remediation or official vendor-recommended mitigation must be deployed within **72 hours** of discovery.
- **High Risk (CVSS 7.0-8.9):** Remediation must be completed within **14 calendar days**.
- **Medium / Low Risk:** Remediation shall be scheduled into the standard monthly patching cycle.

3. **Staging Validation & Production Windows:** Security patches must undergo compatibility and regression testing within a dedicated Staging environment on the first Wednesday of every month. Approved patches shall be deployed to Production environments during off-peak maintenance windows (02:00-05:00 AM UTC) on the second Wednesday of the month, following advance operational notice.

PDF+ 1

2.7 Audit Logging, SIEM, and Immutable Storage

1. **Mandatory Event Logging Scope:** Application and infrastructure logging agents must continuously record:

PDF

- All player wagering transactions (bets, wins, deposits, withdrawals)

.

PDF

- Random Number Generator (RNG) output logs, seed changes, and Jackpot trigger events.

PDF

- Administrator authentication, privilege escalation, and system configuration modifications.

PDF

- Database queries executing bulk data exports or schema alterations.

2. **Log Standardisation and SIEM Streaming:** All logs must be structured into JSON format and streamed in real time to a centralized Security Information and Event Management (SIEM) cluster.

PDF

3. **Immutable WORM Archiving:** Production log archives must be synchronized daily to cloud storage buckets configured in Write-Once-Read-Many (WORM) mode (e.g., AWS S3 Object Lock). Log deletion or modification permissions must be cryptographically restricted from all accounts, including Root/Global Admin, for a mandatory retention period of **5 years**.

PDF+ 1

4. **Real-Time SOC Escalation:** The SIEM system must maintain automated alert triggers for anomalous behavioral patterns (e.g., >5 failed administrative logins in 60 seconds, unauthorized database modifications, or single-transaction payouts exceeding defined threshold limits), escalating instantly to the on-call engineer via PagerDuty.

2.8 Network Perimeter, Email, and Endpoint Defense

1. **Protective DNS Filtering:** Corporate network gateways and enterprise endpoints must route all DNS queries through protective DNS resolvers (e.g., Cloudflare Teams, Cisco Umbrella) to dynamically block command-and-control (C2) domains, malware distribution sites, and phishing portals.

PDF

2. **Endpoint Detection and Response (EDR):** Centralized EDR agents (e.g., CrowdStrike, SentinelOne) must be deployed across 100% of servers and employee workstations. EDR agents must operate in "Auto-Quarantine" mode to isolate process threats automatically. Endpoints missing active EDR telemetry for mor

e than 72 hours shall be revoked network access.

PDF

3. **USB Storage Execution Restrictions:** Group Policies must enforce the absolute disablement of USB mass-storage autorun capabilities and write permissions across all enterprise workstations. Official external file transfers must strictly utilize corporate encrypted cloud storage.

PDF

2.9 Business Continuity, Backups, and Disaster Recovery

1. Automated Backup Schedules:

- **Core Gaming Databases & Ledger Systems:** Real-time Write-Ahead Logging (WAL) replication + hourly immutable snapshots + daily full backups.

PDF

- **Application Configurations & OS Baselines:** Automated daily backups.

2. **3-2-1 Backup Strategy & Encryption:** Backup datasets must be maintained across 3 distinct copies, utilizing 2 different storage media types, with 1 off-site copy stored in a geographically distinct secondary cloud region (e.g., Primary: AWS Tokyo; Secondary: GCP Singapore). All backup archives must be encrypted using AES-256.

PDF+ 1

3. **Air-Gapped Ransomware Defenses:** Off-site backup buckets must operate on dedicated, logically air-gapped IAM tenants with Immutable Snapshot protection enabled to ensure recoverability in the event of primary domain ransomware compromise.

PDF

4. **Bi-Annual Disaster Recovery (DR) Drills:** The DR taskforce shall execute a live system recovery simulation every April and October in an isolated sandbox environment. Drills must validate achieving a Recovery Time Objective (RTO < 4 hours) and Recovery Point Objective (RPO < 15 minutes). All performance metrics must be documented in a signed *DR Simulation Audit Report*.

PDF

2.10 Third-Party (B2B) Ecosystem and Feed Oversight

1. **Vendor Risk Management (TPRM):** Compliance shall maintain an active registry of all third-party B2B providers, game content studios, payment gateways, and sports data feed vendors. Third-party vendors must submit valid ISO/IEC 27001 or GLI certifications prior to onboarding, subject to annual re-evaluation.

PDF+ 1

2. **Data Feed & API Cryptographic Verification:** Integrations providing live sports data feeds, odds, or external game results must enforce Mutual TLS (mTLS) authentication and HMAC API message signing. API Gateways must evaluate incoming data logic; out-of-bounds parameter anomalies must automatically trigger an immediate **Market Suspension** across affected wagering modules.

PDF+ 1

3. **B2B Certification Lapse Protocols:**

- Compliance officers shall review the CGA licensing register monthly to verify the standing of all active B2B partners.

PDF

- B2B commercial agreements must legally bind providers to notify the Company within **12 hours** of any regulatory suspension, certification lapse, or scope modification.

PDF

- **Immediate Suspension Mandate:** Upon receiving notification or discovering a B2B certification lapse, IT Operations shall **disable all API routing endpoints for the affected B2B provider within 2 hours** and submit an immediate formal notification to the CGA.

PDF

2.11 Incident Management and Mandatory 24-Hour CGA Reporting

1. **Incident Severity Matrix:**

- **Priority 1 (Critical):** Outages affecting core wagering systems (>30 minutes), confirmed data breaches involving PII/financial ledgers, RNG/Jackpot exploits, or failure of CGA regulatory reporting feeds.

PDF

- **Priority 2/3 (Moderate/Minor):** Non-critical operational degradation, isolated workstation malware infections successfully contained by ED R.

2. **P1 Response Escalation:** Detection of a P1 incident triggers immediate Pager Duty alerts, assembling an emergency War Room comprising the CISO, CCO, IT Infrastructure Lead, Legal Counsel, and CEO.

PDF

3. **Mandatory 24-Hour CGA Notification SOP:**

- Pursuant to LOK Article 5, for any incident that impacts system availability, game fairness, player fund security, or data privacy, the Compliance Officer **MUST formally notify the Curaçao Gaming Authority within 24 hours of incident confirmation.**

PDF

- The initial notification must detail: (a) Nature and root cause of the incident; (b) Estimated impact on operations and player data; (c)

Immediate containment actions taken; and (d) Timeline for full remediation.

PDF

- Concealing an incident or failing to notify the CGA within the mandatory 24-hour window constitutes a severe license breach, subjecting responsible personnel to immediate termination and legal prosecution.

PDF

2.12 Physical Security, Personnel Vetting, and Security Governance

1. **Personnel Vetting Standards:** All prospective employees must execute non-disclosure agreements (NDAs) prior to receiving system access. Personnel candidate selections for sensitive roles (including Finance, Database Administration, Systems Engineering, and Compliance) must undergo rigorous pre-employment background screening, covering criminal history and financial credit checks.

PDF+ 1

2. **Physical Security Controls:** Physical server rooms, network closets, and surveillance monitoring centers must enforce dual-factor access control (smart card + biometric verification), logging all entries for a minimum of 2 years. Continuous 24/7 CCTV surveillance must cover all rack spaces and access perimeters, with video archives retained for at least 90 calendar days.

PDF+ 1

3. **Security Awareness and Phishing Simulations:** All onboarding employees must complete baseline cybersecurity training within 3 days of joining. The SOC shall execute unannounced, simulated phishing campaigns quarterly via platforms such as KnowBe4. Employees who fail two simulated campaigns within a 12-month period must undergo mandatory remedial training and face performance score deductions.

PDF+ 1

4. **Audit and Compliance Governance:** The Executive Compliance Committee shall convene quarterly to review organizational security metrics, vulnerability remediation SLA compliance, and regulatory alignment. The Company shall engage a CGA-approved independent auditing firm annually to conduct comprehensive Penetration Testing and ISMS compliance audits.

PDF+ 1

3. ENFORCEMENT, PENALTIES, AND LEGAL INDEMNIFICATION

1. **Internal Disciplinary Action:** Strict compliance with this policy is mandatory. Any employee, contractor, or vendor who deliberately circumvents security

ty controls, shares administrative credentials, installs unauthorized software, or conceals a cybersecurity incident shall be subject to immediate disciplinary proceedings, up to and including summary dismissal for cause and civil litigation.

PDF+ 1

2. **Regulatory Indemnification:** In the event that an employee's gross negligence, willful misconduct, or unauthorized actions directly cause regulatory sanctions, administrative financial penalties, or the suspension/revocation of the gaming license issued to Aquarius Entertainment N.V. by the Curaçao Gaming Authority, **the Company reserves the right to pursue full civil indemnification and legal damages against the responsible individual(s) to the maximum extent permitted by law.**

PDF

4. DOCUMENT REVISION AND AUTHORIZATION

This policy document shall be formally reviewed by the Compliance Department on an annual basis or immediately following significant structural, technical, or regulatory changes issued by the CGA.

PDF

- **Document Drafted By:** Security & Compliance Governance Taskforce, Aquarius Entertainment N.V.
- **Reviewed & Approved By:** Chief Information Security Officer (CISO) & Chief Compliance Officer (CCO)
- **Final Authorization:** Board of Directors / Chief Executive Officer, Aquarius Entertainment N.V.